DATA PROTECTION POLICY

1. Introduction

This Policy sets out the obligations of Box Marketing Limited, a company registered in the United Kingdom under number 04900452, whose registered office is at 2-4 Packhorse Road, Gerrards Cross, Buckinghamshire, England, SL9 7QE ("the Company") regarding data protection and the rights of Box Marketing employees, Clients, Business Contacts and Suppliers ("data subjects") in respect of their personal data under UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018.

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be.

2.1. Processed lawfully, fairly, and in a transparent manner in relation to the data subject

2.2. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

2.3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.4. Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

2.5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.

2.6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

3.1. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3.2. The right to be informed

3.3. The right of access

3.4. The right to rectification

3.5. The right to erasure (also known as the 'right to be forgotten')

3.6. The right to restrict processing

3.7. The right to data portability

3.8. The right to object; and

3.9. Rights with respect to automated decision-making and profiling.

Should any employee wish to exercise any of these rights they should e-mail yourdataGDPR@fieldsalessolutions.com

4. Lawful, Fair, and Transparent Data Processing

4.1. The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

4.1.1. The data subject has given consent to the processing of their personal data for one or more specific purposes.
4.1.2. The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them.
4.1.3. The processing is necessary for compliance with a legal obligation to which the data controller is subject.
4.1.4. The processing is necessary to protect the vital interests of the data subject or of another natural person.
4.1.5. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
4.1.6. The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental

rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4.2. If the personal data in question is "special category data" (also known as "sensitive personal data") (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

4.2.1. The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless UK GDPR law prohibits them from doing so).
4.2.2. The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by UK GDPR law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
4.2.3. The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
4.2.4. The processing relates to personal data which is clearly made public by the data subject.
4.2.5. The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity.
4.2.6. The processing is necessary for substantial public interest reasons, on the basis of UK GDPR law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.
4.2.7. The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of UK GDPR law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR; or
4.2.8. The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of UK GDPR law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy).

5. Specified, Explicit, and Legitimate Purposes

5.1. The Company collects and processes the personal data set out in the relevant privacy notice.

5.2. The Company only collects, processes, and holds personal data for the specific purposes set out in the relevant privacy notice (or for other purposes expressly permitted by the GDPR).

5.3. Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data.

6. Accuracy of Data and Keeping Data Up to Date

6.1. The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up to date. This includes, but is not limited to, the rectification of personal data at the request of a data subject.

6.2. The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

6.3. ' Need to ensure that your personal details are up to date and accurate. When you first start working for us' we record your name, address, next of kin and contact telephone details. In the event that any of these change you should contact your line manager in the first instance. You will be invited to review and update personal information on a regular basis

7. Data Retention

7.1. The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

7.2. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

7.3. For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

8. Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 11 to 16 of this Policy.

9. Accountability and Record-Keeping

9.1. The Business Process Manager shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

9.2. The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

9.2.1. The name and details of the Company and any applicable third-party data processors.
9.2.2. The purposes for which the Company collects, holds, and processes personal data.
9.2.3. Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates.
9.2.4. Details of any transfers of personal data to non-UK or non-EEA countries including all mechanisms and security safeguards.
9.2.5. Details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy); and
9.2.6. Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

10. Data Protection Impact Assessments

10.1. The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

10.1.1. Data Protection Impact Assessments shall be overseen by the Business Process Manager and shall address the following:
10.1.2. The type(s) of personal data that will be collected, held, and processed.
10.1.3. The purpose(s) for which personal data is to be used.
10.1.4. The Company's objectives.
10.1.5. How personal data is to be used.
10.1.6. The parties (internal and/or external) who are to be consulted.
10.1.7. The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed.
10.1.8. Risks posed to data subjects.
10.1.9. Risks posed both within and to the Company; and
10.1.10. Proposed measures to minimise and handle identified risks.

11. Data Security - Transferring Personal Data and Communications

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

11.1.1. All emails containing personal data will be encrypted where possible. All e-mails must be checked prior to sending and the use of OneDrive must be considered as an alternative.

11.2. All emails containing personal data must be marked "confidential".

11.3. Personal data may only be transmitted over secure networks.

11.4. Personal data may not be transmitted over a public network.

11.4.1. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted.

11.4.2. Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it.

11.4.3. Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using Special Delivery.

11.4.4. All personal data transferred physically should be transferred in a suitable container marked "confidential".

12. Data Security – Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data: All electronic copies of personal data should be stored securely using passwords.

12.1.1. All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely.

12.1.2. All personal data stored electronically should be backed up daily with backups stored on local storage in Thame office and in our dedicated secure backup environment in our data centre in Manchester (off-site).

12.1.3. No personal data should be stored on any mobile device, whether such device belongs to the Company or otherwise without the formal written approval from yourdata@GDPR@fieldsalessolutions.com and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary and;

12.1.4. No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);

13. Data Security – Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company's Data Retention Policy.

14. Data Security - Use of Personal Data

14.1.1. The Company shall ensure that the following measures are taken with respect to the use of personal data:

14.1.2. No personal data may be shared informally and employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the yourdataGDPR@fieldsalessolutions.com;

14.1.3. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation.

14.1.4. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time.

14.1.5. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and

14.1.6. Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Business Services Manager to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

15. Data Security - IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security:

15.1.1. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Company is designed to require such passwords.

15.1.2. All software (including, but not limited to, applications and operating systems) shall be kept up to date. The Company's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and

15.1.3. No software may be installed on any Company-owned computer or device without the prior approval of the ICT department.

16. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

16.1.1. All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy and shall be provided with a copy of this Policy.

16.1.2. Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company.

16.1.3. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.

16.1.4. All employees, agents, contractors, or other parties working on behalf of the Company handling data will be appropriately supervised.

16.1.5. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise.

16.1.6. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.

16.1.7. All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy.

16.1.8. The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.

16.1.9. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract.

16.1.10. All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the GDPR; and

16.1.11. Where any agent, contractor or other party working on behalf of the Company handling personal data in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

17. Transferring Personal Data to a Country Outside the UK

The Company may from time-to-time transfer ('transfer' includes making available remotely) personal data to countries outside of the UK.

17.1.1. The transfer of personal data to a country outside of the UK shall take place only if one or more of the following applies:

17.1.2. The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the UK GDPR governing body has determined ensures an adequate level of protection for personal data.

17.1.3. The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the UK GDPR governing body; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

17.2. The transfer is made with the informed consent of the relevant data subject(s).

17.2.1. The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject).

17.3. The transfer is necessary for important public interest reasons.

17.4. The transfer is necessary for the conduct of legal claims.

17.4.1. The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

17.4.2. The transfer is made from a register that, under UK law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

18. Data Breach Notification

18.1.1. All personal data breaches must be reported immediately to yourdataGDPR@fieldsalessolutions.com.

18.1.2. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Business Services Manager must

ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

18.1.3. In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 18.2) to the rights and freedoms of data subjects, the Business Services Manager must ensure that all affected data subjects are informed of the breach directly and without undue delay.

18.2. Data breach notifications shall include the following information:

18.2.1. The categories and approximate number of data subjects concerned.
18.2.2. The categories and approximate number of personal data records concerned.
18.2.3. The name and contact details of the Company's contact point where more information can be obtained.
18.2.4. The likely consequences of the breach.
18.2.5. Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Implementation of Policy

This Policy has been approved and authorised by:

Name:	Julian Cordy
Position:	Chief Executive Officer
Date:	24th May 2018
Date reviewed:	

Reviewed 25th May 2019
Reviewed June 2020
Reviewed June 2021
Reviewed September 2022